**UNITED STATES DISTRICT COURT**
**WESTERN DISTRICT OF MICHIGAN**
**SOUTHERN DIVISION**

**1:23-cv-842**
**Hala Y. Jarbou**
**U.S. Chief District Judge**

DAVID ANGEL SIFUENTES III,
Plaintiff,

CASE NO.
HONORABLE:

**FILED - KZ**
August 11, 2023 2:00 PM
U.S. DISTRICT COURT
WESTERN DISTRICT OF MICHIGAN
mg Scanned by 8/11/23

V.

ADOBE,
Defendant.

DEMAND FOR JURY TRIAL

_____/

## COMPLAINT AND MEMORANDUM OF LAW

Now comes, the Plaintiff David Angel Sifuentes III, In Pro Se and submits this complaint and memorandum of law and demand or jury trial seeking relief for identity theft via data breach, personal information being exposed, along with, password stolen from a data breach from Adobe, this Court has diversity jurisdiction of state law claims as Sifuentes is a citizen of Michigan and Adobe is a citizen of California. Sifuentes has standing to bring this complaint. *See In re Zappos.com, Inc., 884 F.3d 893 (9th Cir. 2018), Galaria v. Nationwide Mutual Insurance Co. No., 663 F.App'x 384 (6th Cir. 2016),* California deceptive trade practices act, California legal remedies act, California unfair competition law, Michigan Consumers Protection Act against deceptive trade practices, invasion of privacy by public disclosure of private facts, negligence per se, breach of fiduciary duty, unjust enrichment, breach of implied contract, negligence, negligent and or intentional infliction of emotional distress, conversion (use of information without permission) breach of bailment, failure to provide safeguard security measures and protection to Sifuentes for the breach, and risk of future injury. Sifuentes is seeking damages of $300,000.00 in damages and punitive damages of $250,000,000.00 for a total of $250,300,000.

Sifuentes ask this Court to liberally construe his pleadings, legal documents, arguments and not fault him for not citing are applying the correct case law, statute and applicable laws under *Haines v. Kerner, 404 U.S. 519 (1972).* Pro se litigants can be excused from full compliance with technical procedural rule, provided there is substantial compliance. *Norefleet v. Walker, 684 F.3d 688 (7th Cir. 2012).* Court and staff have a special responsibility to scrutinize carefully pro se

complaints. *Chapman v. Kleindienst, 507 F.2d 1246, 1253 (7th Cir. 1974)* (district court has responsibility for finding hidden jury demands in the middle of complaints). ). A court must accept all allegations of well-plead factual allegations as true, *League Am. Citizens v. Bredesen, 500 F.3d 523, 527 (6th Cir. 2007)*, and factual allegations alone is what matters. *Albert v. Carovano, 851 F.2d 561, 571 n.3 (2nd Cir. 1988)*.

***Jurisdiction***

This court has ***both personal and diversity jurisdiction*** under this complaint, This court has diversity Jurisdiction Sifuentes is a citizen of Grand Rapids, Michigan and Adobe is a citizen of San Jose, California a cooperation headquartered at 345 Park Ave, San Jose, CA 95110, and therefore the parties are different citizens and this court has jurisdiction of all civil matters. *See Wis. Dep't of Corr. v. Schacht, 524 U.S. 381, 388 (1998),* also since California is the principal place of business for Adobe where they are headquartered. *Hertz Corp. v. Friend, 559 U.S. 77 (2010)*as the damages are more than $75,000 28 U.S.C. § 1332. Sifuentes is seeking damages of $300,000.00 and punitive damages of $35,000,000 which can also be added for jurisdictional purposes. *Hayes v. Equitable Energy Res. Co., 226 F3d 560 (6th Cir. 2001).* This court also has personal jurisdiction under the "minimum contacts" rule as Sifuentes received services from Adobe being an account via online in Michigan. Pursuant to MCL 600.711, a Michigan court may exercise general personal jurisdiction over a defendant-corporation if: (1) it is incorporated under the laws of Michigan; (2) the defendant has consented to personal jurisdiction in Michigan; or (3) the corporation "carr[ies] on… a continuous and systematic part of its general business within the state."

Michigan's long-arm statute "has been construed as conferring on the state courts the maximum scope of personal jurisdiction consistent with due process." *Amway Corporation v. Kope Food Products, Inc., 840 F. Supp. 78, 80 (W.D. Mich. 1993).* The exercise of limited jurisdiction "occurs where 'a State exercises jurisdiction over a defendant in a suit arising out of or related to the defendant's contacts with the forum.'" *Kmart Corp. v. Key Industries, Inc., 877 F. Supp. 1048, 1051 (E.D. Mich. 1994), quoting Nacionales de Colombia, S.A. v. Hall, 466 U.S. 408, 414 n. 9 (1984)*. Michigan extends limited jurisdiction over nonresident corporations pursuant to MCL § 600.715. Pursuant to Michigan's Long Arm Statute, MCL 600.715, "a

sufficient basis of jurisdiction to enable a court of record of this state to exercise limited personal jurisdiction" exists when a corporation's acts "create any of the following relationships: (1)[t]he transaction of any business within the state" or "(2) [t]he doing or causing an act to be done, or consequences to occur, in the state resulting in an action for tort." In interpreting MCL 600.715, the Michigan Supreme Court has held that "[t]he word 'any' means just what it says. It includes 'each' and 'every.' It comprehends 'the slightest.'" *Sifers v Horen 385 Mich 195, 199 n 2, 188 NW2d 623 (1971).*

***Facts***

On are around November 2022 Sifuentes obtained a report from Credit Karma and informing him that his personal information was comprised from Adobe. Sifuentes did not contact Adobe about the breach. Sifuentes opened an Adobe account between 2009-2010, in regards of their services needed to read documents and also download flash players and other Adobe products for Adobe failed to secure and protect through careless security and negligence personal information concerning Sifuentes personal information such as the email address, davidsifuentes61@yahoo.com and password which he used for other accounts. Further facts may be presented in this pleading. The breach occurred sometime in 2013 according to a Experian dark web scan Sifuentes personal information such as emails and passwords which he used for numerous accounts, the same one used with Adobe, which is "fairly traceable" to the breach Adobe had on file such as his email and password he has been using.

***STANDARD OF REVIEW***

A data breach victim may seek relief in Federal Court when a company has failed to protect the data of its customers. See *Galaria v. Nationwide Mutual Insurance Co., 663 F.App'x 384 (6th Cir. 2016).* This includes heightened risk of future injury, *In re U.S. Office of Personnel Management Data, 928 F.3d 42 (D.C. Cir. 2019).* A litigant need not provide proof of monetary damage to bring a claim of data breach in Federal Court. A plaintiff threatened with future injury has standing to sue "if the threatened injury is 'certainly impending,' or the risk that the harm will occur. See *In re Zappos.com, Inc., 884 F.3d 893 (9th Cir. 2018).* A litigant need only

provide *concrete proof* that his personal information had been comprised by the breach. See *Transunion LLC v. Ramirez, 141 S.Ct. 2190 (2021).*

***Timing***

Sifuentes claims are timely under "***common law and California delayed discovery rule***". *Cada v. Baxter Healthcare Corp., 920 F.2d 446, 450 (7th Cir. 1990); California Sansome Co. v. U.S. Gypsum, 55 F.3d 1402 (9th Cir. 1995).* Also under Michigan, law MCL 600.5805. Although the data breach occurred in 2012, Sifuentes took reasonable steps of investigating the matter once she was put on notice of the and learned of the severability of the breach. Also discovery of fraud is applicable in this matter, *Merck & co. v. Reynolds, 559 U.S. 633, 644 (2010): Cf: Rotkiske v. Klemm, 140 S.CT. 355 (2019), MCL 440.2201,* where Adobe took no action and covered up the breach, no notification was ever sent to Sifuentes to notify him of the breach. Sifuentes claims are timely under Michigan, law MCL 600.5805. Equitable tolling is applicable to all of Sifuentes claims as he was never notified by Adobe of the breach and is tolled, as he has been exercising due diligence in the investigation of his claims, MCL 600.5856, and still suffers harm of the breach where his personal information where it is "fairly traceable" his personal information from Adobe had been on the dark web. Sifuentes personal information was stolen and was supposed to be protected Adobe has a duty to protect all sensitive data which they neglected to do so in this matter.

***Judicial Notice***

Pursuant to Fed. R. Evid. 201(c)(2), the Court "must take judicial notice if a party requests it and the court is supplied with the necessary information." Types of facts that may be judicially noticed include those that "can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned." Fed.R.Evid. 201(b)(2). This includes materials that are in the public record. *New England Health Care Employees Pension Fund v. Ernst & Young, LLP, 336 F.3d 495, 501 (6th Cir. 2003)*("A court that is ruling on Rule 12(b) motion may consider materials in addition to the complaint if such materials are public records or are otherwise appropriate for the taking of judicial notice."); *Rodic v. Thistledown Racing Club, Inc.,*

*615 F.3d 736, 738 (6th Cir. 1980)* ("Federal courts may take judicial notice of proceedings in other courts of record."). Sifuentes ask that this Court take judicial notice of Exhibits A Adobe email, and also the following articles discussed on the effects and worth of data.

***The effects and worth of data.***

Sifuentes ask that this Honorable Court take judicial notice of the following public online articles in support of his complaint. Data personal identifier information (PII) is very valuable and priceless as there is unlimited potential for cybercriminal's to do harm. PII is valuable property. See Articles online Marc Van Lieshout, *The Value of Personal Data at p. 4, 457 IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 26 (MAY 10, 2015)*, available at https://researchgate.net/publication/283668023_The_Value_of_Personal_Data 9"The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible[.]") (last visited August 8, 2023).

Companies such as Adobe profit from data used from Adobe Firms are able to attain significant market valuations by employing business models predicated on the successful use or personal data within the existing regulatory and legal frameworks. See *Exploring the Economics of Personal Data: A Survey of methodologies for Measuring Monetary Value, OECD Digital Economic Papers no. 220 (Apr. 2, 2013),* https://www.oecd-ilibrary.org/science-and-technology/exploring-the economics-of-personal-data_5k486qtxldmq-en (last visited April 11, 2023). See *U.S. Firms to Spend Nearly $19.2 billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017,* INTERACTIVE ADVERSTISING BUREAU (De. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/ (last visited August 8, 2023).

PII can be sold from anywhere from $40 to $200, and bank details have a price range of $50 to $200. Anita George, *Your personal data is for sale on the dark web*. Here's how much it costs, Digital Trends (Oct. 16, 2019), https://www/digitaltrends.com/computing/peronsal-data-sold-on -the-dark-web-how-much-it-costs/ (last visited April 11, 2023). Criminals can also purchase entire data breaches from $900 to $4,500. In the Dark, VPNOveriew.com, 2019, https://vpnoveriew.com/privacy/anonymous-browsing/in-the-dark/ (last accessed on April 4, 2023). Experian has found that stolen debit and credit cards details can sell for $5 to $110 on the dark web. Brian Stack, Here's How Much Your Personal Information is Selling fro on the Dark

Web, Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited August 8, 2023).

Adobe collects and sells information concerning phone plans and other personal information concerning consumers and there habits, as consumers place a high value on the privacy of that data. There has been research that sheds light on how much consumers value their data privacy-and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites. Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011),* https://www.jstor.org/stable/23015560?seq=1 (last visited August 8, 2023). Cyberattacks have become so frequent that the U.S. Secret Service and FBI have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals…because they often have a lesser IT defenses and a high incentive to regain access to their data quickly. Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware, LAW360 (Nov. 18, 2019)*, https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransonmware (last visited August 8, 2023).

Data is very valuable and criminals have a need to use that property that is individuals PII.

***I. Deceptive trade practices, legal remedies, unfair competition law, consumer protection act against deceptive trade practices.***

Adobe has violated the California deceptive trade practices act, legal remedies act, and unfair competition law and Michigan Consumer protection Act for not providing adequate protection of Sifuentes personal data information stored with Adobe.

Here Adobe deprived Sifuentes of the security measures and procedural protections also adequate process to protect his personal information. Sifuentes personal information his identity that is facts that represent his reputation have been taken and could be used to commit future crimes and create imminent danger and risk. On or about November 2022 Sifuentes found that he was a victim of a data breach from Adobe (See Exhibit "A") notifying him that his data PII

personal information had been compromised. A data breach victim may seek relief in Federal Court when a company has failed to protect the data of its customers. See *Galaria v. Nationwide Mutual Insurance Co., 663 F.App'x 384 (6th Cir. 2016).* This includes heightened risk of future injury, *In re U.S. Office of Personnel Management Data, 928 F.3d 42 (D.C. Cir. 2019).* A litigant need not provide proof of monetary damage to bring a claim of data breach in Federal Court. A plaintiff threatened with future injury has standing to sue "if the threatened injury is 'certainly impending,' or the risk that the harm will occur. See *In re Zappos.com, Inc., 884 F.3d 893 (9th Cir. 2018).* A litigant need only provide *concrete proof* that his personal information had been comprised by the breach. See *Transunion LLC v. Ramirez, 141 S.Ct. 2190 (2021).*

Sifuentes has shown in injury in fact and concrete injury of the data breach where his identity has been stolen that is his personal data and information from Adobe which includes his name, and private facts, such information can and has been comprised which leads to hackers using the data to commit crime are assume the Identity of Sifuentes that is identity theft a concrete injury, *Transunion LLC, v. Ramirez, 141 S.Ct. 2190 (2021); Galaria v. Nationwide Mutual Insurance Co. No., 663 F.App'x 384 (6th Cir. 2016); Clemens v. ExecuPharm Inc., 48 F.4th 146 (3rd Cir. 2022)*:

Article III standing requires a plaintiff to demonstrate." (1) that he or she suffered an injury in fact that is concrete, particularized, and actual or imminent, (2) that the injury was caused by the defendant, and (3) that the injury would likely be redressed by the requested judicial relief. this court does not have jurisdiction and his state law claims should proceed in federal court.Id., citing cases.

Here the data breach occurred that is theft of Sifuentes identity, two the injury-in-fact is actual or imminent as the data from Adobe that is personal facts still and endure the kind of future harm that qualifies as 'imminent." *Clemens v. ExecuPharm Inc., 48 F.4th 146, 152 (3rd Cir. 2022).* The data could be used to open bank accounts and other accounts and commit crime that is cybercrimes with it.

***II. Invasion of privacy, negligence negligence per se, breach of fiduciary duty, unjust enrichment, breach of implied contract, negligence, negligent and or intentional infliction of emotional distress, conversion (use of information without permission) breach of bailment, failure to provide safeguard security measures and protection to Sifuentes for the breach, and risk of future injury, violation of California and Michigan data breach laws.***

Sifuentes has suffered invasion of privacy by public disclosure of private facts where his personal information has been stolen and taken without him knowing and without permission. Sifuentes is going through negligent and intentional infliction of emotional distress as his personal information has been stolen for nearly 14 years plenty of time for hackers and cyber criminals to cause harm, in the hands of cyber criminals. The Adobe information can be used to obtain personal accounts read email from gmail and intercept personal information which exposes his social security number and banking account information from other banks. This is stressful and Sifuentes is very mad and scared as hackers can commit crimes with his personal information and payment information available. Sifuentes information is also on the dark web. Adobe was negligent and had careless security, measures. Sifuentes is going through negligent and intentional infliction of emotional distress as his personal information had been stolen. Adobe 'intentionally, willfully, recklessly, or negligently" failed to take sufficient measures to safeguard the data, and follow the guidelines of the Federal Trade Commission. In fact, it is "fairly traceable" cyber criminals have had access to Sifuentes data from Adobe. Sifuentes is scared as hackers can commit crimes with his personal information and credit card information. Sifuentes information is also on the dark web.

Adobe duties rise from California and Michigan deceptive trade practices and unfair competition law and Michigan Consumer protection act prohibiting deceptive practices, which prohibits "unfair… practices in or affecting commerce," including, as interpreted by California and Michigan, the unfair act or practice by a business, such as Adobe, of failing to employ reasonable measures to protect and secure PII.

Adobe violated California's deceptive trade practices and unfair methods of competition and or deceptive acts or practices prohibited act and Michigan Consumer protection act prohibiting deceptive practices by failing to use reasonable measures to protect Sifuentes and all other users affected by the breach, and not complying with applicable industry standards. Adobe's conduct was particularly unreasonable given the nature and amount of PII it obtains and stores, and the foreseeable consequences of data breach involving PII including, specifically, the substantial damages that would result to Sifuentes. Adobe violations of these acts constitutes negligence per se.

Sifuentes and users either directly or indirectly gave Adobe their PII in confidence, believing that Adobe would protect that information. Sifuentes and users would not have provided Adobe with this information had they known it would not be adequately protected. Adobe acceptance and storage of Sifuentes's created a fiduciary relationship between Adobe and Sifuentes. In light of this relationship, Adobe must act primarily for the benefit of its customers, which includes safeguarding and protecting Sifuentes's PII.

Adobe has a fiduciary duty to act for the benefit of Sifuentes and upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Sifuentes's and users PII, failing to comply with the data security guidelines set forth by California deceptive trade practices and unfair methods of competition and or deceptive acts or practices prohibited act and Michigan Consumer protection act prohibiting deceptive practices, and otherwise failing to safeguard the PII it collected and collects.

Data is a business and Adobe collects a monetary benefit upon users, and selling data. Adobe accepted or had knowledge of the benefits conferred upon it by Sifuentes. Adobe also benefited from the receipt of Sifuentes and Adobe users. Sifuentes paid for phone service and provided financial information for his phone account.

As a result of Adobe's conduct, Sifuentes suffered actual damages in an amount equal to the difference in value between his valuable data used to make profit made with reasonable data privacy and security practices and procedures that Sifuentes and other customer's paying Adobe users without reasonable data privacy and security practices and procedures that they received.

Adobe required Sifuentes and users to provide, or authorize the transfer of, their PII in order for Adobe to provide services. Adobe entered into implied contracts with Sifuentes in which Adobe agreed to comply with its statutory and common law duties to protect Sifuentes's PII and to timely notify him in the event of a data breach.

Sifuentes would not have provided his PII to Adobe had he known that Adobe would not safeguard his PII, as promised, or provide timely notice of a data breach or any notice of all such as in this case.

Emails are linked to Sifuentes other accounts, such as Gmail which he submits personal information. This is private and no one would know personnel facts of Sifuentes concerning the info in Adobe which contains his dating profile and personal private information.

Sifuentes is seeking $300,000.00 for actual damages for injuries caused by negligent intentional infliction of emotional distress such as being very mad, angry, and sacred, worried, nervous and has trouble sleeping and scared of what else hackers stole and can steal from his information, *Buchholz v. Meyer Njus Tanick, PA, 946 F. 3d 855 (6th Cir. 2020)*, and will do as they keep accessing his accounts and his information is in the dark web damages for intentional infliction for these acts and future acts or appropriate in this matter. See e.g. *Greta L. Anderson v. American Airlines, 352 Fed.Appx. 182 (9th Cir. 2009); Baker v. Johnson Morrell & Co., 266 F.Supp.2d (N.D. Iowa 2003); Morgan v. New York life Insurance co., 559 f.3d 425, 443 (6th Cir. 2009)*. Sifuentes reserves the right to assert and clarify additional claims.

Adobe is in violation of conversion that is unauthorized assumption and exercise of the right of ownership over goods or personal data belonging to Sifuentes. The data breach was an unauthorized act depriving Sifuentes of his personal property that is his PII with Adobe.

This was inconsistent violation of conversion wrongful exercise of Sifuentes personal property that is his PII.

These acts are breach of bailment, failure to notify promptly of the breach and provide security measures and Protection to Sifuentes for the breach. The data is Sifuentes personal property that he entrusted and had stored with Adobe. As discussed Adobe has an express duty to take care of their account holders, under applicable state and federal laws. See Cal civil Code Sec. 1798.81.5(d)(1)(A); 1798.82;1798.29; MCL 445.72.

Adobe has violated California and Michigan data breach laws Cal civil Code Sec. 1798.81.5(d)(1)(A); 1798.82;1798.29, MCL 445.72, by failure to personally notify Sifuentes and other data breach victims and follow security procedures.

Sifuentes seeks $250,000,000.00 in exemplary, economic and noneconomic damages compensatory and punitive damages injunctive and declaratory relief as this is calculated from the fines and penalties associated from companies concealing data breaches from victims such as the Equifax data breach which settled for around $575,000,000, *In re: Equifax, Inc. Customer Data Security Breach litigation, Case no. 1:17-md-2800-TWT (N.D. Ga.)*, for failing to take action with data breach protocols. See e.g. *Philip Morris USA v. Williams, 549 U.S. 346 (2007)*. Also the $190 data breach settlement of Capital One.

Sifuentes ask that this honorable court not fault him for citing, interpreting or applying any incorrect law to this matter, *Haines v. Kerner, 404 U.S. 519 (1972),* but place him in the correct legal label and theory, *Castro v. U.S., 540 U.S. 375 (2003).*

## RELIEF REQUESTED

**WHEREFORE,** Sifuentes **PRAYS** that this Honorable court grant relief as follows:

Award Sifuentes $300,000.00 in actual damages for negligent and intentional infliction of ongoing emotional distress for being mad upset and under stress and $250,000,000.00 in exemplary, compensatory and punitive damages injunctive and declaratory relief, for a total of $250,300,000 or in the alternative Award $250,000.00 in actual damages and that Adobe provide Sifuentes with 5 years of LifeLock to help clean and restore Sifuentes identity.

Respectfully submitted,

By:_____

Plaintiff In Pro Se
David Angel Sifuentes III
439 More St. NE
Grand Rapids, MI 49503
(616)283-5215
davidsifuentes61@yahoo.com

DATED: August 8, 2023

David Angel Situenteo TJ
439 More St NE
Unit 2
Grand Rapids, MI 49503

Retail

UNITED STATES POSTAL SERVICE

49007

RDC 99

U.S. POSTAGE PAID
FCM LG ENV
GRAND RAPIDS, MI 49501
AUG 09, 2023

$2.07

R2304M109975-12

Clerk
107 Federal Bldg,
410 W Michigan Ave,
Kalamazoo, MI 49007